CONSENSYS

PROJECT KHOKHA CASE STUDY

Pushing the Limits of Interbank Payment Settlement with Blockchain

Project Khokha is an Enterprise Ethereum solution pioneered by the South African Reserve Bank increasing transaction volume and network resilience while maintaining confidentiality requirements for real-time gross settlement

Our goal with Project Khokha is to contribute to the global initiatives which assess the application and use cases of distributed ledger technology (DLT) through this collaborative effort piloted by the South African Reserve Bank (SARB) together with the national banking community."

—Francois Groepe,
Deputy Governor,
South African Reserve Bank

Reimagining Central Banking with Blockchain

For the banking industry, the cost of providing the utmost reliability, availability, and resilience against attacks or equipment failure is high. These costs are further increased by the inefficiency of reconciliation payments and the antiquated reporting processes for suspicious transactions. The South African Reserve Bank (SARB), in partnership with ConsenSys Solutions and seven commercial banks, utilized Quorum, an Enterprise Ethereum solution — in combination with the Istanbul Byzantine Fault Tolerance consensus mechanism, Pedersen commitments, and range proofs — to process the typical daily volume of payments for the South African Reserve Bank, with full confidentiality and finality, in less than two hours.

PROBLEM STATEMENT

How can central banks increase the resiliency of interbank payment systems while maintaining or reducing the overall cost of those systems? The SARB sought to replicate interbank clearing and settlements by deploying a permissioned blockchain network. This exercise was made to assess whether blockchain technology could significantly improve the performance, scale, and confidentiality of payments in a real-world simulation.

SOLUTION

In consortium with seven commercial banks, the SARB partnered with ConsenSys Solutions to build a proof-of-concept grounded in real-world performance, confidentiality requirements, and diverse bank hardware on the blockchain without a single point of failure.

GOALS ACHIEVED

1. 70,000 transactions executed in less than two hours. This rate achieved the transaction performance target, condensing one business day's worth of transaction processing time by 75%.
2. 95% of block prorogation time in <1 second and 99% propagation in <2 seconds. This demonstrated that acceptable performance is achievable, despite the geographical distribution of the banks' hardware.
3. Maintained full privacy while meeting required transaction volumes. This was the first time that the IBFT consensus mechanism, Pedersen commitments, and range proofs for confidentiality were used with Quorum. Together these solutions delivered unprecedented scalability, resilience, confidentiality, and settlement finality.

Project Khokha was recognized by the Central Bank Publication as the "Best Distributed Ledger Initiative" of 2018.

Problem Statement Story

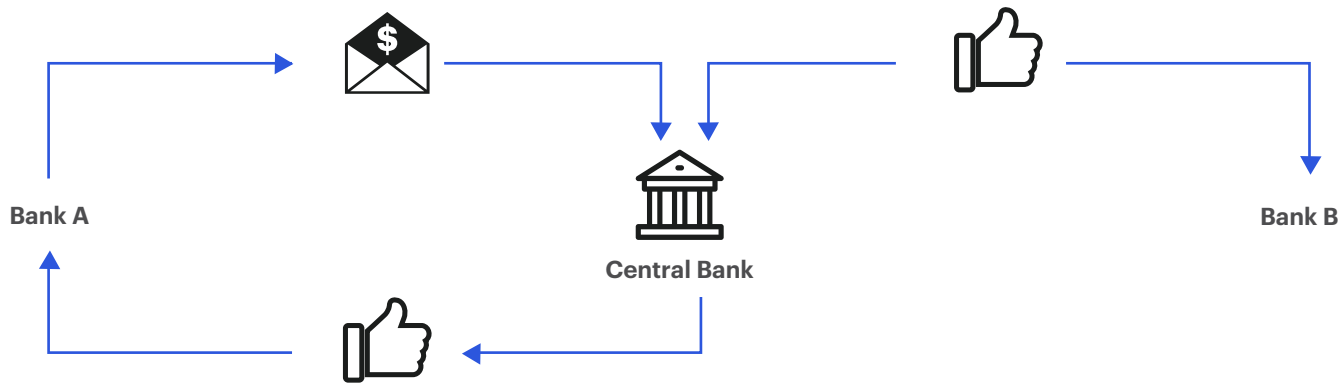
Investigating more resilient and cost-effective wholesale payment systems

Interbank payments are critical for every country, and each bank has a mandate to protect the financial interests of its country. However, the ongoing cost of resilience is steep. If a central bank's servers go down, regional banks would not be able to pay one another, leaving the country's payment clearing system to collapse. To prevent this scenario, central banks invest substantial capital in infrastructure and security. Blockchain technology now presents a comparatively secure, efficient, and cost-effective alternative. If every bank were to use blockchain technology, no bank would have a single point of failure. Essentially, a country could maintain its interbank payment network even if one or several nodes were down.

Bank reconciliation is an intrinsically inefficient process. A study by EY reports that an overwhelming 59% percent of total finance and actuarial costs are expended on transaction processing and reporting.

For example, when Bank A needs to make a payment, it sends a message to the Central Bank to make one on its behalf. The Central Bank then sends a message back to Bank A saying they've done so, and notifies the receiver, Bank B, that they've received money from Bank A. Bank A needs a mirror account to keep a record of their holdings at the Central Bank and continuously reconcile transactions against that balance. This single payment requires four transactions to complete. With a blockchain, everything would take place on a distributed network. Since all banks would operate on the same ledger, they would be able to pay one another directly, simplifying the process and largely eliminating the risks of double spending, fraud, and network vulnerability.

INTERBANK PAYMENTS TODAY



INTERBANK PAYMENTS WITH BLOCKCHAIN

Regulatory reporting is another burden that lays with banks. Every bank is obligated to report suspicious transactions and transaction details. However, by leveraging blockchain technology, banks could have access to a distributed ledger that contains all transactions, with details of who paid whom, what sum was exchanged, and when the transaction occurred. With this technology, reporting can be streamlined and automated by pulling data from the ledger. Meanwhile, regulators will have access to data from a single source of truth with near real-time reporting.

ENTERPRISE ETHEREUM SOLUTION

The SARB initiated Project Khokha in the latter part of 2017 to explore interbank wholesale settlement using Distributed Ledger Technology (DLT). The SARB engaged ConsenSys Solutions as its technical partner and worked with a consortium of banks for the project: Absa, Capitec, Discovery Bank, FirstRand, Investec, Nedbank, and Standard Bank.

ConsenSys was selected as the lead partner due to expertise gathered from its previous blockchain in banking projects, including Project Ubin with the Monetary Authority of Singapore (MAS). Knowledge gained from ConsenSys' role as architect and technology partner spearheading the integration of the Quorum workstream for Project Ubin enabled Project Khokha to take off quickly.

BUILDING A SMARTER SOLUTION WITH BLOCKCHAIN

This initiative consisted of three 'waves' of work. Wave 1 created a proof-of-concept on the Ethereum blockchain. Wave 2 investigated the interconnected issues of scalability, resilience, confidentiality, and finality. It was during this stage that the scope of Project Khokha became more clearly defined. Project Khokha was designed to provide a realistic test of a DLT-based wholesale payments system. In particular, it investigated whether confidentiality could be achieved at scale. Wave 3 will diverge into areas such as securities settlement and cross-border transactions.

Project Khokha is the first implementation of Quorum with the Istanbul Byzantine Fault Tolerance (IBFT) and Pedersen commitments to create a distributed ledger between participating banks. The tokenization of the South African Rand (ZAR) enabled a domestic payment system that allowed participating banks to pledge, redeem, and track balances on the blockchain without a centralized central bank system— that is, without a single point of failure. This combination of technologies provided robust confidentiality while permitting the transaction throughput required.

Once Project Khokha achieved its targets for performance, scalability, resilience, confidentiality, and settlement finality, the team shifted its focus to the sharing of know your customer (KYC) and anti-money laundering (AML) payment information between banks, as well as the Financial Intelligence Center (FIC), by enabling these actors to decrypt relevant transaction data.

THE PROJECT KHOKHA QUORUM SOLUTION USED SEVERAL FINALITY, PRIVACY, AND CONFIDENTIALITY MECHANISMS.

1. The Istanbul Byzantine Fault Tolerance

The Istanbul Byzantine Fault Tolerance is a consensus mechanism in an Ethereum network. Like other consensus algorithms, IBFT ensures a single, agreed-upon ordering for transactions on the blockchain, but provides additional benefits for enterprises, including increased throughput and settlement finality.

2. Whisper for private messaging

A secure peer-to-peer messaging system built into Ethereum. At the start-up of the network, each bank exchanges encryption keys with every other bank via this channel which are then used in transactions between said banks. The SARB keeps a copy of all keys to view all transactions.

3. Pedersen commitments

Proven to be effective in ensuring full confidentiality of transaction amounts, Pedersen commitments allow the sender of a payment to commit to a value without being able to change it once the commitment is provided. Pedersen commitments are perfectly hiding and computationally binding under the discrete logarithm assumption.

4. Range proofs

Range proofs are a type of zero-knowledge proof that enables one party to prove that a secret value (like one contained in a Pedersen commitment) is within a certain numerical range.

GOALS ACHIEVED

Pushing new boundaries to achieve privacy with required transaction volumes

Project Khokha offers a significant contribution to the global DLT body of knowledge with record-setting results and the first time combined utilization of the IBFT consensus mechanism, Pedersen commitments, and Quorum. This project demonstrated that the typical daily volume of the South African payments system could be processed in less than two hours with full confidentiality of transactions— a record time with such specifications. IBFT, Pedersen Commitments, and range proofs delivered a solid combination of scalability, resilience, confidentiality, and finality.

Project Khokha demonstrated the practical test of a network across diverse bank hardware, pushing new boundaries in terms of confidentiality and performance in a regulated environment.

The aim of Project Khokha was not to replace the SARB's standing interbank settlement system, SAMOS, but to evaluate the use case of distributed ledger technology in wholesale payments for interbank settlements. The success of Project Khokha is compounded by the potential to apply its learnings to future blockchain in banking initiatives. The SARB has joined other central banks around the world that are leveraging emerging technology to find innovative solutions.

Project Khokha received the 'Best Distributed Ledger Initiative' award from Central Banking Publications in 2018. It was a significant step forward for Enterprise Ethereum and Quorum, showcasing in one use case just how much the banking industry stands to benefit from blockchain technology.

TECHNOLOGY PARTNERSHIPS

ADHARA

ABOUT ADHARA

Adhara, a ConsenSys spoke, enables liquidity management and international payments for decentralized finance networks. The team, led by Peter Munnings, provided the technical horsepower behind Project Khokha.

For more information, visit www.adhara.io

Quorum

ABOUT QUORUM

Quorum is an enterprise focused version of Ethereum. It is an open-source blockchain platform that combines the innovation of the public Ethereum community with enhancements to support enterprise needs such as privacy, strong permissions, and high performance.

For more information, visit www.goquorum.com

CONSENSYS

This system can be developed to enable other uses beyond wholesale settlement. Examples include the exchange of tokenized money for other tokenized assets, like bonds or securities..”

— SARB